SHUMAKER LOOP & KENDRICK LLP
Terence S. Reynolds
treynolds@shumaker.com
Lucas D. Garber
lgarber@shumaker.com
101 South Tyron Street
Suite 2200
Charlotte, North Carolina 28280
Telephone: (704) 375-0057
Facsimile: (704) 332-1197
Local Civil Rule 83.1(d) Counsel for Plaintiff Jason Williams

PIERCE BAINBRIDGE BECK PRICE & HECHT LLP
Christopher LaVigne
clavigne@piercebainbridge.com
Dwayne Sam
dsam@piercebainbridge.com
Sarah Baugh
sbaugh@piercebainbridge.com
Thomas Popejoy
tlpopejoy@piercebainbridge.com
277 Park Avenue, 45th Floor
New York, NY 10172
Telephone: (212) 484-9866
Facsimile: (646) 968-4125
(pro hac vice forthcoming)
Counsel for Plaintiff Jason Williams

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
EASTERN DIVISION
Case No. 4:19-cv-00153

JASON WILLIAMS,

Plaintiff,

v.

AT&T MOBILITY, LLC,

Defendant.

CIVIL COMPLAINT

DEMAND FOR JURY TRIAL

I. NATURE OF THE ACTION

1. This action arises out of AT&T's repeated failure to protect its wireless cell service subscriber—Jason Williams—from the negligence and/or purposeful actions of its own employees, resulting in massive and ongoing violations of Mr. Williams's privacy, the compromise of his highly sensitive personal and financial information, ongoing and egregious threats to the safety of his family, and the collapse of a business in which Mr. Williams had invested over $2 million.

2. AT&T is the country's largest wireless service provider. Tens of millions of subscribers entrust AT&T with access to their confidential information, including information that can serve as a key to unlock subscribers' highly sensitive personal and financial information.

3. Recognizing the harms that arise when wireless subscribers' personal information is accessed, disclosed, or used without their consent, federal and state laws require AT&T to protect this sensitive information.

4. AT&T also recognizes the sensitivity of this data, and promises its subscribers that it will protect and safeguard their accounts from unauthorized access and use.

5. In an egregious violation of the law and its own promises, and despite advertising itself as a leader in technological development and as a cyber security-savvy company, AT&T repeatedly breached its duty to Mr. Williams to protect his account and the sensitive data it contained. AT&T failed to implement sufficient data security systems and procedures and failed to supervise its own personnel, instead standing by as its employees negligently and/or purposefully helped third-party hackers gain unauthorized access to his account in order to rob, extort, and threaten him and his associates.

6. Mr. Williams brings this action to hold AT&T accountable for its violations of federal and state law, and to recover for the grave financial and personal harms suffered by Mr. Williams, his business and his family as a direct result of AT&T's acts and omissions, as detailed herein.

II. THE PARTIES

7. Plaintiff Jason Williams is, and at all relevant times was, a resident of North Carolina. Mr. Williams currently resides in Raleigh, Wake County, North Carolina, with his wife and three young daughters.

8. Mr. Williams is a co-founder and partner at Morgan Creek Digital, a highly successful asset management firm in North Carolina that invests in blockchain technologies and the digital assets industry. Mr. Williams is a well-known entrepreneur—having started his first business at age 23—and was an early cryptocurrency investor and enthusiast. He has a significant social media presence, where he frequently discusses cryptocurrency news and developments.

9. Until February of 2019, Mr. Williams operated a large-scale bitcoin "mining" business. Mr. Williams invested over $2 million—including $1.4 million in specialized mining hardware—in what was a profitable and successful business prior to the negligence and actions of AT&T.

10. Mr. Williams is a former AT&T wireless customer. He purchased a wireless cell phone plan from AT&T in Raleigh, Wake County, North Carolina in approximately 2000 for personal use and was an active, paying AT&T wireless subscriber until February 2019.

11. Defendant AT&T Mobility, LLC (referred to herein as "AT&T") is a Delaware limited liability corporation with its principal office or place of business in Brookhaven, Georgia. AT&T Mobility provides wireless service to subscribers in the United States, Puerto Rico, and the U.S. Virgin Islands. AT&T "provides nationwide wireless services to consumers and wholesale and resale wireless

subscribers located in the United States or U.S. territories" and transacts or has transacted business in this District and throughout the United States. It is the second largest wireless carrier in the United States, with more than 153 million subscribers, earning $71 billion in total operating revenues in 2017 and $71 billion in 2018.[1] As of August 2019, AT&T has 130 stores in North Carolina, including 11stores in Raleigh, North Carolina.[2]

12. AT&T is a "common carrier" governed by the Federal Communications Act ("FCA"), 47 U.S.C. § 151 *et seq.* AT&T is regulated by the Federal Communications Commission ("FCC") for its acts and practices, including those occurring in this District. AT&T transacts or has transacted business in this District and throughout the United States.

13. AT&T Inc., AT&T's parent company, acknowledged in its 2018 Annual Report that its "profits and cash flow are largely driven by [its] Mobility business" and "nearly half of [the] company's EBITDA (earnings before interest, taxes, depreciation and amortization) comes from Mobility."[3]

14. Despite the importance of its mobility business, instead of focusing on ramping up security for their customers, AT&T Inc. has gone on a buying spree costing over $150 billion, acquiring: Bell South (including Cingular Wireless and Yellowpages.com), Dobson Communications, Edge Wireless, Cellular One, Centennial, Wayport, Qualcomm Spectrum, Leap Wireless, DirecTV, and Iusacell and NII Holdings (now AT&T Mexico). During the same period, AT&T's mobile phone business was rated as the worst among major providers. Consumer Reports named it the "worst carrier" in 2010, and the next year, J.D. Power found AT&T's

[1] *2018 Annual Report*, AT&T, https://investors.att.com/~/media/Files/A/ATT-IR/financial-reports/annual-reports/2018/complete-2018-annual-report.pdf.
[2] *Stores/North Carolina*, AT&T, https://www.att.com/stores/. Unless otherwise indicated, all URLs in this complaint were last accessed on October 22, 2019.
[3] *Id.*

network the least reliable in the country—a dubious achievement that it also earned in prior years. Little wonder that its customers were the least happy of subscribers of the Big Four carriers according to the American Consumer Index. In the meantime, AT&T Inc. has purchased, for a total equity value of $85.4 billion, Time Warner Inc.—the owner of HBO, Warner Bros, CNN, Turner Broadcasting, Cartoon Network, Turner Classic Movies, TBS, TNT and Turner Sports.

III. JURISDICTION AND VENUE

15. This Court has jurisdiction over this matter under 28 U.S.C. § 1331 because this case arises under federal question jurisdiction under the Federal Communications Act ("FCA"). The Court has supplemental jurisdiction under 28 U.S.C. § 1367 over the state law claims because the claims are derived from a common nucleus of operative facts. The Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1332 because Mr. Williams is a citizen of a different state than AT&T.

16. This Court has personal jurisdiction over AT&T because AT&T purposefully directs its conduct at North Carolina, transacts substantial business in North Carolina (including in this District), has substantial aggregate contacts with North Carolina (including in this District), engaged and is engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons in North Carolina (including in this District), and purposely avails itself of the laws of North Carolina. AT&T's website claims that "AT&T has invested in [] North Carolina communications networks, [] people and local communities for 139 years."[4] AT&T's presence in North Carolina gave rise to the injuries suffered by Mr. Williams, as alleged in this Complaint: Mr. Williams purchased his AT&T wireless plan in North Carolina, visited AT&T retail locations

[4] *AT&T North Carolina*, AT&T, https://engage.att.com/north_carolina/.

in North Carolina, and was injured in North Carolina by the acts and omissions alleged herein.

17. In accordance with 28 U.S.C. § 1391, venue is proper in this District because a substantial part of the conduct giving rise to Mr. Williams' claims occurred in this District and Defendant transacts business in this District. Mr. Williams purchased his AT&T wireless plan in this District and was harmed in this District, where he resides, by AT&T's acts and omissions, as detailed herein.

IV. ALLEGATIONS APPLICABLE TO ALL COUNTS

18. As a telecommunications carrier, AT&T is entrusted with the sensitive wireless account information and personal data of millions of Americans, including Mr. Williams' confidential and sensitive personal and account information.

19. Despite its representations to its customers and its obligations under the law, AT&T has failed to protect Mr. Williams' confidential information.

20. On multiple occasions between November 2018 and February 2019, third-party hackers, through the assistance and/or negligence of AT&T employees, obtained unauthorized access to Mr. Williams AT&T wireless account, viewed his confidential and proprietary personal information, and transferred control over Mr. Williams AT&T wireless number from Mr. Williams' phone to a phone controlled by the third-party hackers. The hackers and employees then utilized their control over Mr. Williams' AT&T wireless number—including control secured through cooperation with and/or the negligence of AT&T employees—to steal his and his family's personal and private information and threaten his family, and to access his personal and digital finance accounts, steal his cryptocurrency, and destroy his business, all resulting in the loss of Mr. Williams' $2 million investment. After Mr. Williams' personal information was compromised, he also had to halt his lucrative cryptocurrency mining operations, in order to stop the hackers from stealing more.

21. This type of account hacking behavior is known as "SIM swapping."

A. SIM Swapping is a Type of Identity Theft Involving the Transfer of a Mobile Phone Number.

22. On seven occasions in 2018 and 2019, Mr. Williams was the target of "SIM swapping."

23. "SIM swapping" refers to a relatively simple scheme, wherein third parties take control of a victim's wireless phone number. The hackers then use that phone number as a key to access the victim's digital accounts, such as email, file storage, and financial accounts.

24. Most cell phones, including the iPhone owned by Mr. Williams at the time of his SIM swap, have internal SIM ("subscriber identity module") cards. A SIM card is a small, removable chip that allows a cell phone to communicate with the wireless carrier and the carrier to know what subscriber account is associated with that phone. The connection between the phone and the SIM card is made through the carrier, which associates each SIM card with the physical phone's IMEI ("international mobile equipment identity"), which is akin to the phone's serial number. Without a working SIM card and effective SIM connection, a phone typically cannot send or receive calls or text messages over the carrier network. SIM cards can also store a limited amount of account data, including contacts, text messages, and carrier information, and that data can help identify the subscriber.

25. The SIM card associated with a wireless phone can be changed. If a carrier customer buys a new phone that requires a different sized SIM card, for example, they can associate their wireless account with a new SIM card and the new phone's IMEI by working with their cell phone carrier to effectuate the change. This allows carrier customers to move their wireless number from one cell phone to another and to continue accessing the carrier network when they switch cell phones. For a SIM card change to be effective, the carrier must authenticate

the request and actualize the change. AT&T allows its employees to conduct SIM swaps for its customers remotely or in its retail stores.

26. A SIM swap refers to an unauthorized and illegitimate SIM card change. During a SIM swap attack, the SIM card associated with the victim's wireless account is switched from the victim's phone to a phone controlled by a third party. This effectively moves the victim's wireless phone subscriber identity from their phone to a phone controlled by the third party (also referred to herein as a "hacker"). The hacker's phone then becomes the phone associated with the victim's carrier account, and the hacker receives all of the text messages and phone calls intended for the victim. Meanwhile, the victim's phone loses its connection to the carrier network.

27. Once hackers have control over the victim's phone number, they can use that control to access the victim's personal online accounts, such as email and banking accounts, through exploiting two-factor authentication. Two-factor authentication allows digital accounts to be accessed without a password, or allows the account password to be changed. One common form of two-factor authentication is through text messaging. Rather than enter a password, the hacker requests that a password reset be sent to the mobile phone number associated with the account holder. Because the hacker now controls that phone number, the reset code is sent to the hacker. The hacker can then log into, and change the password for, the victim's account, allowing them to access the contents of the account.

28. The involvement of a SIM swap victim's wireless carrier is critical to an effective SIM swap attack. In order for a SIM swap change to occur and for a SIM swap victim to be at any risk, the carrier must receive a SIM change request and effectuate the transfer of the victim's phone subscriber identity and number from one SIM card to another.

29. In Mr. Williams's case, not only did AT&T authorize changes to his account without Mr. Williams' permission, but—upon information and belief—its employees ignored and even deleted instructions that AT&T informed Mr. Williams that it had placed on his wireless account in order to prevent additional SIM swaps. AT&T also accessed his account without permission and changed his passcode.

B. Prior to the SIM Swap Attacks, Mr. Williams Engaged in Sophisticated and Expensive Cryptocurrency Mining Operations.

30. An early cryptocurrency investor and enthusiast, Mr. Williams is also involved in cryptocurrency mining. Cryptocurrency mining is a process by which new cryptocurrency is introduced into the existing circulating supply, as well as a way to secure the network on which the cryptocurrency operates. Cryptocurrency mining is extremely technologically complex and requires a complicated technical set up as well as large amounts of electrical power.

31. Miners like Mr. Williams introduce new cryptocurrency, such as bitcoin ("bitcoin" or "BTC"), by solving complex computational problems, called cryptographic hash, which allow them to chain together "blocks" of transactions. A transaction that occurs via a cryptocurrency network would be something like "Abby sent 10 coins to Bob." In a block, a large number of these transactions are verified by the miner and then bundled. After all transactions in the block are verified, the miner computes the cryptographic hash. This process takes intense computing power and technological sophistication, as hundreds of millions of calculations are executed each second. Once the miner successfully calculates the hash, the block is relayed to the network to be verified, and the block is added to the blockchain network. Finally, the miner is rewarded with a set amount of the cryptocurrency for his or her work.

32. Since February 2018, Mr. Williams has invested over $2 million in his cryptocurrency mining operation, the bulk of which was spent on servers powerful enough to compute the cryptographic hash required to successfully mine.

33. These servers, which Mr. Williams set up in Virginia, are called cryptocurrency rigs, and consist of specialized hardware sets that are specifically set up to mine cryptocurrency. The purpose of Mr. Williams' rigs was to mine bitcoin, and as they mined, they would place bitcoin rewards in his mobile wallet. He has spent an additional $650,000 in this business, including optimizing the rigs' set up and paying for the electricity to power them.

34. Mr. Williams' efforts were successful. By November 2018, Mr. Williams was successfully mining between seven and twelve bitcoins per month. Each bitcoin was worth approximately $6,381 at the beginning of November 2018, putting Mr. Williams' accumulated bitcoin holdings at approximately $450,000.

C. AT&T Allowed Unauthorized Access to Mr. Williams' Account Seven Times Over the Course of Approximately Four Months.

35. Mr. Williams' sophisticated and successful cryptocurrency mining operation—and the significant investment made to set up that operation—were destroyed by AT&T's failure to protect Mr. Williams' wireless AT&T account, and the data contained therein.

36. Between November 5, 2018 and February 8, 2019, third-party hackers were able to gain access to Mr. Williams' phone on approximately seven occasions by conducting unauthorized SIM swaps on Mr. Williams' AT&T wireless phone. After obtaining control over Mr. Williams' AT&T wireless phone, the hackers were able to gain access to Mr. Williams' personal and financial accounts, including the accounts connected to his mining operations. These SIM swaps, and the resulting harm, would not have been possible but for the participation and negligence of AT&T and its employees.

THE FIRST SIM SWAP ATTACK

37. On November 5, 2018, Mr. Williams was on vacation in Jamaica. At around 11:30 PM, he noticed that his AT&T wireless phone suddenly displayed text reading, "No SIM card" in the upper left corner of the screen. Mr. Williams immediately shut off the phone. He suspected a SIM swap attack was occurring and called AT&T with his wife's phone to try to regain control over his account. Mr. Williams' fears were correct; third party hackers were conducting a SIM swap attack on his AT&T account.

38. Mr. Williams' told AT&T that hackers were trying to gain access to his account, and that AT&T needed to do something to stop the hack from continuing.

39. While Mr. Williams was unable to access and/or use his AT&T wireless number, hackers utilized their control over the number to log into his personal email account, change his account password, and change the cell phone number and email account used for two-step verification from Mr. Williams' number and email to a number and email controlled by the hackers. This effectively eliminated Mr. Williams' ability to log in to his account or to use two-factor authentication to bypass the changed password, solidifying the hackers' control. Utilizing his Gmail account to change passwords, they also hacked into his Twitter, Instagram, DropBox, Google Drive, and LinkedIn accounts.

40. The hackers were also able to create a "mirror image" of his phone, so they could see every app Mr. Williams used on his mobile device. Mr. Williams had various apps to access cryptocurrency exchanges on his mobile device. These exchanges are online platforms where different forms of cryptocurrency (e.g. bitcoin) are bought and sold. By seeing which apps Mr. Williams had on his phone, the hackers were able to figure out that he most likely had money or cryptocurrency on these accounts, and attempt to hack into them.

41. They accessed Mr. Williams' Coinbase account—a cryptocurrency exchange—and changed the password.

42. They also accessed his Slush Pool account. Slush Pool is a cryptocurrency mining platform that accumulates the computing power of individual miners. It allows miners to consolidate computing power and share cryptocurrency rewards. Once the hackers accessed this account, they redirected the bitcoin rewards from Mr. Williams' Slush Pool account to their own cryptocurrency wallet, locked the wallet configuration (which took away Mr. Williams' ability to change it), and denied Mr. Williams access to the interface, stripping him of his access, operation, or control of his mining operation. They also transferred around .23 bitcoin to their bitcoin wallet.[5] These actions compromised all the mining rigs that Mr. Williams had purchased, and all the cryptocurrency rewards were funneled to the hackers.

43. Because the hackers had changed his Slush Pool account to provide rewards to their wallet, Mr. Williams had to reconfigure all his mining rigs in Virginia. He hired a third-party to reconfigure these servers, which took around five days to complete. During this reconfiguration period, Mr. Williams was unable to mine and lost the ability to earn from these rigs.

44. The hackers also compromised highly sensitive personal information contained in Mr. Williams's Gmail account. This personal information included his home address, his and members of his family's social security numbers, copies of their passports, TSA precheck information, sensitive financial documents, and sensitive personal documents, including patents, pending patents, and various intellectual property concepts and ideas.

[5] At that time, Bitcoin was worth around $6,446.00 per unit, so hackers stole around $1,500.00 worth of BTC from him.

45. The hackers then used this highly sensitive personal information to extort Mr. Williams. In November 2018, an unknown party texted Mr. Williams and told him that if he did not respond to their threats, they would sell his information on the dark web on a hacker exchange website. Mr. Williams did not respond to their threats.

46. While hackers were busy robbing Mr. Williams and destroying his mining business, AT&T employees were on the phone with Mr. Williams attempting to address the issue. Eventually, an employee at the AT&T store sent a recovery email to Mr. Williams' wife's email account, allowing Mr. Williams to regain control of his AT&T wireless phone number.

47. Following the first SIM swap attack, Mr. Williams contacted AT&T and asked what measures AT&T could take to stop this from happening again. AT&T represented that it would add extra security to Mr. Williams' account by making changes and notations in his account, whereby the SIM card associated with his account could only be changed via an in-person request in a specific, identified Raleigh AT&T store. Additionally, AT&T represented that Mr. Williams' identity would have to be confirmed with two passports before AT&T would approve a SIM card change on his account. Further, Mr. Williams informed AT&T employees at that time that he was a financial manager involved with cryptocurrency trading, and that he was at a heightened risk of SIM swap attacks. On reliance on AT&T's representations that it would add extra security to his account, Mr. Williams decided not to close his AT&T wireless account.

48. Shortly after the first SIM swap attack, Mr. Williams began receiving threats on his AT&T wireless account number. On November 28, 2018, at approximately 3:40 PM, Mr. Williams and his family were at home when Mr. Williams began receiving threatening text messages from an unfamiliar phone number with a California area code. The texts contained Mr. Williams' name,

home address, and social security number—information obtained by hackers, on information and belief, as a result of the SIM swap attack. The text threatened Mr. Williams' wife and daughter, and attempted to extort him for money. Mr. Williams received another text later the same evening from the same number, again threatening his daughter.

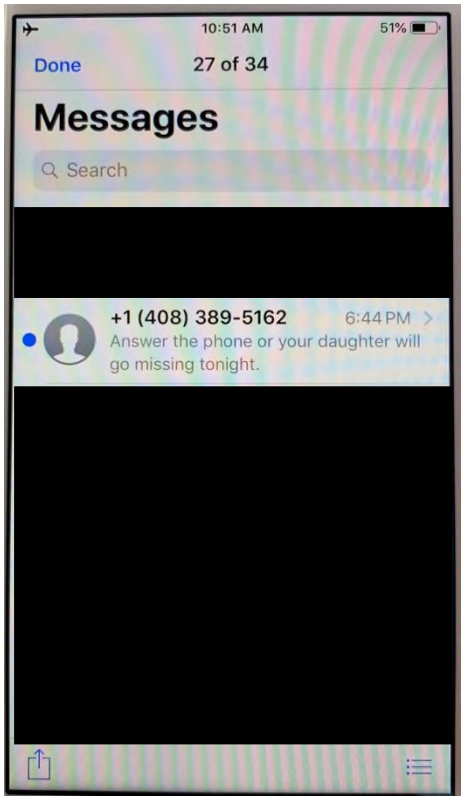

Figure 1

49. Mr. Williams and his family were terrified, and he called the FBI and the local police. The local police department said there was nothing they could do to protect Mr. Williams and his family, except add more neighborhood patrols. They asked Mr. Williams if he had a concealed carry license and, when he said he did, they encouraged Mr. Williams to carry a gun with him at all times. Mr. Williams had never regularly carried a gun with him before the SIM swap attack. However, after he received these texts, he began to carry guns with him at all times in order to ensure the safety of himself and his family. He also began to stay up all

night to watch the outside of his home to ensure no intruders or nefarious individuals came around.

THE SECOND SIM SWAP ATTACK

50. Despite AT&T's representations that Mr. Williams' account would be safe from unauthorized SIM swaps and that the company had put robust security protocols in place to protect his account, Mr. Williams was the victim of another SIM swap attack less than one month later, on November 30, 2018.

51. Mr. Williams was at home, and suddenly received multiple texts from AT&T that said, "AT&T currently trouble shooting your phone." He immediately called AT&T and warned the company that someone was trying to hack his phone via a SIM swap attack. While Mr. Williams was on the phone with AT&T trying to prevent additional damage and maintain control over his AT&T wireless account, his cell phone lost service as the result of the SIM swap attack.

52. During this attack, the hackers attempted to access Mr. Williams' Gemini account and locked him out of his Gmail account again.[6] Mr. Williams immediately went to the designated store with two passports to reverse the SIM swap. While he was at the AT&T store, Mr. Williams was told that an AT&T employee named Steve helped an individual claiming to be Mr. Williams effectuate a SIM swap attack. The individual pretending to be Mr. Williams was able to swap Mr. Williams' SIM despite only providing a fake driver's license as verification of his identity, which was a direct violation of AT&T's representations that Mr. Williams' SIM card could not be changed absent identity verification in the form of two valid passports.

[6] Gemini is a cryptocurrency exchange platform similar to Coinbase.

THE THIRD SIM SWAP ATTACK

53. On December 1, 2018, the very next day, Mr. Williams was SIM swapped again.

54. Mr. Williams was in Greensboro, North Carolina, attending a soccer tournament and noticed around 4:00 PM that his AT&T wireless phone had lost service. He immediately suspected another SIM Swap.

55. During this attack, the hackers again attempted to access his Gemini account and locked him out of his Gmail account.

56. Later that night, at approximately 9:55 PM, Mr. Williams received a text from an unfamiliar phone number that said "Hello Jason Williams." At 2:53 AM the next morning and at 2:25 PM the next day, he received two more text messages: "Hello?" and "You have until today to respond or all hell will be let loose."

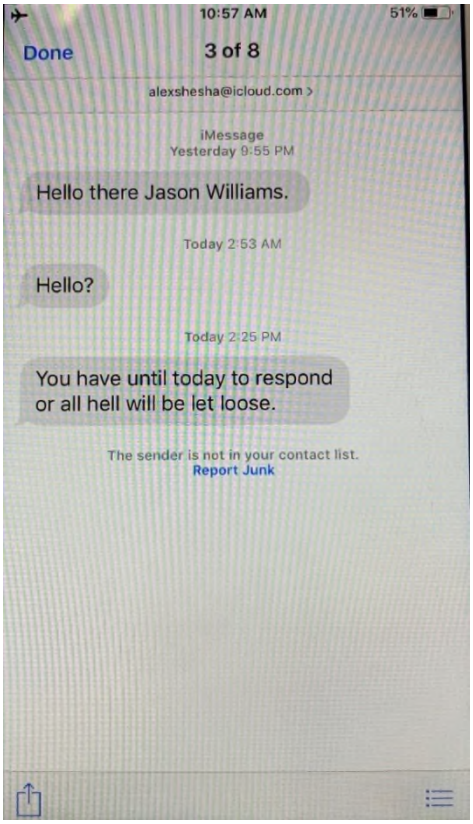

Figure 2

57. On December 2, 2018, Mr. Williams went into a designated AT&T store in Raleigh with two passports. He disabled his SIM Card and bought a new iPhone for around $700. He purchased the new iPhone because AT&T employees told him it would mitigate the risk of another SIM swap attack.[7] An AT&T employee assisting Mr. Williams showed him a warning message in his account directing AT&T employees not to change the SIM card associated with Mr. Williams' account unless he requested the change in-person, at a specific and identified AT&T retail store, with two passports verifying his identity.

58. When Mr. Williams told the AT&T employee about the multiple attacks, the AT&T employee said the warnings must be getting deleted from his AT&T account. The AT&T employee also told him he was on a special list of individuals who were at high risk of being SIM swapped.

THE FOURTH SIM SWAP ATTACK

59. That very same evening, upon returning from the AT&T retail store, Mr. Williams was SIM swapped again. He noticed the attack was happening when he suddenly had no cell phone service and could only connect to WiFi.

60. Like the other attacks, the hackers attempted to gain access to his Gemini account and his Gmail account.

61. By utilizing their control over Mr. Williams' AT&T cell phone number, the hackers also accessed Mr. Williams' Twitter account through two-factor authentication associated with his phone number. Mr. Williams has tens of thousands of Twitter followers, many of whom follow him because of his involvement with and knowledge of cryptocurrency. Via Twitter, the hackers contacted Mr. Williams' friends and business associates, impersonated him, and

[7] Mr. Williams later contacted AT&T asking them why the new phone would mitigate a SIM swap risk, but AT&T never responded.

asked that they send “Mr. Williams” cryptocurrency, thereby stealing money from Mr. Williams’ friends and associates and causing professional and reputational damage to Mr. Williams.

62. When Mr. Williams discovered this hack, he turned around and went back to the AT&T store with his two passports and reversed the SIM swap.

63. While Mr. Williams worked with AT&T to regain control over his AT&T wireless account, he again asked about the warnings placed on his account that AT&T represented would prevent future SIM swap attacks. The AT&T representative with whom Mr. Williams spoke informed him that the warnings were erased from his account, but could not provide any explanation as to why.

64. On December 5, 2018, Mr. Williams went to the designated AT&T store in Raleigh to discuss this latest SIM swap attack with AT&T employees. He asked AT&T employees at the store to confirm that there was a note in his account that AT&T should not effectuate a SIM card change unless Mr. Williams asked in person at the designated AT&T retail store with two passports. The AT&T employees confirmed there was a note in his account regarding SIM swap procedures.

65. Mr. Williams was understandably and visibly upset about the ongoing breaches of his privacy, safety, and security. He showed the AT&T employees screenshots of the threats he had been receiving, which caused them grave concern. Rather than assist Mr. Williams, an AT&T employee called the local police. When the police officers arrived, Mr. Williams told them about his situation, including the threats against himself and his family, and the police again encouraged him to carry a gun.

THE FIFTH SIM SWAP ATTACK

66. Despite AT&T's repeated representations that his AT&T wireless account was safe, Mr. Williams' AT&T wireless account was breached and his SIM card swapped without his authorization for a *fifth* time on February 4, 2019.

67. Mr. Williams was in Islamorada, Florida, at the time of this hack. At approximately 9:30 PM, he noticed his SIM card was deactivated.

68. He contacted AT&T and asked them to immediately disable his phone so the hackers would not have service.

69. Before the phone was disabled, and while the hackers had control over Mr. Williams' AT&T wireless number, they used that control to access Mr. Williams' accounts on various cryptocurrency exchange platforms, including his Coinbase and Gemini accounts.

70. The hackers also again solicited cryptocurrency from Mr. Williams' friends and associates on Twitter by utilizing their control over his cell phone number to gain access to his Twitter account. Mr. Williams immediately flew back to North Carolina to address this hack, incurring additional expense as a result.

71. On February 5, 2019, Mr. Williams went to the designated Raleigh AT&T retail store to recover his AT&T wireless account. AT&T employees informed him that his SIM card had been swapped the night before via email after an online representative changed his four-digit pin password. After each SIM swap incident, Mr. Williams changed his four-digit pin password, yet he continued to be hacked. During this specific hack, Mr. Williams was able to find out that an online AT&T representative changed his four-digit pin for the hacker.

THE SIXTH SIM SWAP ATTACK

72. Less than 24 hours later, on February 6, 2019, at around 1:30 AM, Mr. Williams was SIM swapped again. He once again noticed that he suddenly lost AT&T service and was only able to connect to WiFi. He attempted to contact

AT&T, but he had to wait until AT&T's fraud department opened at 8 AM the next morning.

73. During the time he was unable to gain access to his phone, hackers deleted his Slush Pool account, essentially making his mining rigs useless. His Gemini account was also frozen, and hackers attempted to steal 51 BTC.

74. On the evening of February 6, 2019, Mr. Williams went to the designated Raleigh AT&T retail store, and was assisted by two AT&T employees named Jessica and Hassan. Jessica helped him restore his phone and get another SIM card. She also phoned the Fraud Department, who informed her that Mr. Williams' four-digit PIN password was changed online at around 12:36 AM on February 6, 2018, and then two minutes later his SIM card was swapped for "technical reasons."

75. The SIM card was changed over the phone by Rex Mostoles (employee ID RX8927). Mr. Mostoles swapped Mr. Williams' SIM card despite a note in his account information in large, red font that stated AT&T employees were not to make any account changes via phone call or email.

76. Because of this hack, Mr. Williams had no choice but to shut down his mining rigs. These rigs consisted of 500 servers, which cost $2,830.00 each. Mr. Williams realized he had no other option but to terminate mining operations, as AT&T repeatedly failed to keep his mobile device safe. Even if he reconfigured these mines a second time (like he did after the first SIM swap attack), there was no way to ensure the rewards they were mining would not be hacked again. Because of AT&T's failure to adequately safeguard his information, he lost his $1.4 million investment in these servers.

77. Further, besides the loss of his investment, another effect of AT&T's actions was that Mr. Williams lost the ability to mine bitcoin after February 2019. In February 2019, he was mining around 5-9 BTC per month. After he was forced

to shut down his mines, he lost huge amounts of potential profits from bitcoin because he could no longer mine it.

THE SEVENTH SIM SWAP ATTACK

78. On February 8, 2019, Mr. Williams' phone was hacked again. According to the AT&T Fraud Department, his SIM card was swapped at 1:26 AM. An AT&T employee named Vennessa, with user ID VL828B, assisted the hacker. Like the previous SIM swaps, Mr. Williams suspected he was getting SIM swapped after noticing that he suddenly lost AT&T service and was only able to connect to WiFi.

79. After this SIM swap, on February 8, 2019, and February 12, 2019, hackers transferred money totaling $6,500 from his First Citizens bank account to his Coinbase account and bought cryptocurrency. When Mr. Williams realized this was occurring, he drained his First Citizens' bank account so the hackers could not transfer any more money into his Coinbase account.[8]

80. On February 8, 2019, Mr. Williams visited the designated AT&T store around 10:30 AM. Mr. Williams purchased a new SIM card and was able to regain control over his AT&T wireless account. He also informed AT&T he was going to change providers. The associates at the AT&T store told him that because he had recently purchased a new iPhone from AT&T, he was not eligible to unlock it, and utilize the new phone he had bought mere months before. Instead, he would need to go to a new carrier, buy a new iPhone, and port his phone number to that carrier.

81. Mr. Williams immediately went to the Verizon store, purchased a new phone for the second time in two months, and had his number ported over.

[8] To this day, Mr. Williams does not have access to his Coinbase account.

THE EFFECTS OF THE ATTACKS

82. The SIM swaps have exposed Mr. Williams and his family to ongoing threats of physical harms and extortion attempts, as well as personal anguish and distress. Because his phone number has been widely disseminated by the hackers, Mr. Williams no longer answers any calls on his cell phone unless the number is in his contacts, and does not have voicemail capabilities.

83. Mr. Williams' accounts, including his Gmail, HItBTC, Coinbase, Gemini, Slush Pool, LinkedIn, Twitter, and Instagram accounts, were all compromised by the third-party hackers. These accounts contained highly sensitive and confidential personal, legal, and business information. All this data and information has been compromised as a result of the SIM swaps.

84. This includes color copies of his family's passports, their social security numbers, their TSA numbers, password and log-in information for additional accounts, and confidential financial, business, and legal information.

85. Mr. Williams also writes patents, and had proprietary data associated with these patents on his Gmail account. This very valuable and confidential data was compromised when hackers utilized their control over Mr. Williams' AT&T wireless number to access his email account.

86. This information, as well as the additional compromised personal information, is now at a high risk of being posted or bought and sold on the dark web by criminals and identity thieves, putting Mr. Williams, his wife, and his three young children at ongoing risk of significant privacy violations, extortion, identity theft, and countless unknown harms.

87. After each SIM swap, Mr. Williams would try and figure out what happened, what data and accounts had been compromised, and how to mitigate the damages.

88. Mr. Williams and his family have had their personal lives uprooted as a result of the repeated SIM swaps and the resulting privacy violations. They no longer feel safe in their home and feel instable and anxious. Mr. Williams has three young daughters, and they are very scared about the situation. Mr. Williams had to undertake the difficult task of explaining the theft to his children, who now express fear of hackers and robbers and feelings of instability. Though Mr. Williams and his wife tried to shield them from the SIM swap attacks and the associated threats, hackers sent messages to family group chats, and the police had to come to the Williams' home. His young children are terrified about bad things happening to them.

89. Mr. Williams has personally experienced immense harm as a result of the SIM swaps. He has suffered from anxiety, loss of sleep, and extreme depression.

90. Mr. Williams was damaged financially by these hacks as well. Besides the loss of his $1.4 million investment in servers plus the approximately $600,000 in costs, he lost the ability to mine BTC profitably for himself. The mining rigs Mr. Williams purchased for himself are only usable for a certain amount of time, before a combination of technologically-advanced servers being released to the market and the increasing difficulty of BTC mining renders the servers useless. As a result of the unauthorized SIM swaps, Mr. Williams was unable to continue mining BTC during that time period.

D. AT&T's Repeated Failures to Protect Mr. Williams' Account from Unauthorized Access Are a Violation of Federal Law.

91. AT&T is the world's largest telecommunications company and provider of mobile telephone services. As a common carrier,[9] AT&T is governed

[9] 47 U.S.C. § 153(51).

by the Federal Communications Act of 1934, as amended ("FCA"),[10] and corresponding regulations passed by the FCC.[11]

92. Recognizing the sensitivity of data collected by cell carriers, Congress, through the FCA, requires AT&T to protect Mr. Williams' sensitive personal information to which it has access as a result of its unique position as a telecommunications carrier.[12]

93. Section 222 of the FCA, which became part of the Act in 1996, requires AT&T to protect the privacy and security of information about its customers. Likewise, Section 201(b) of the Act requires AT&T's practices related to the collection of information from its customers to be "just and reasonable" and declares unlawful any practice that is unjust or unreasonable.[13]

94. AT&T's most specific obligations to protect its customers concerns a specific type of information, called Customer Proprietary Network Information ("CPNI").[14] Specifically, the FCA "requires telecommunications carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure."[15]

95. Carriers like AT&T are liable for failures to protect their customers unauthorized disclosures.[16] The FCC has also stated that "[t]o the extent that a carrier's failure to take reasonable precautions renders private customer

[10] 47 U.S.C. § 151 *et seq.*
[11] 47 C.F.R. § 64.2001 *et seq.*
[12] 47 U.S.C. § 222.
[13] 47 U.S.C. § 201(b).
[14] 47 U.S.C. § 222(a).
[15] Report and Order and Further Notice of Proposed Rulemaking, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 F.C.C. Rcd. 6927 ¶ 1 (Apr. 2, 2007) (hereafter, "2007 CPNI Order").
[16] 47 U.S.C. §§ 206, 207.

information unprotected or results in disclosure of individually identifiable CPNI, . . . a violation of section 222 may have occurred."[17]

96. CPNI is defined as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and . . . information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."[18]

97. Mr. Williams' CPNI was breached by AT&T employees when they accessed his account and swapped his SIM card without authorization.

98. At least six of the times employees accessed Mr. Williams' account, there was a large note in his account warning employees *not* to conduct a SIM swap unless Mr. Williams requested it in person, at the Raleigh North Hills AT&T store, with two passports.

99. AT&T, through its employees, purposefully and/or with negligence, allowed Mr. Williams SIM card to be swapped *seven* times in four months.

100. Each time his SIM card was swapped, Mr. Williams' CPNI was visible to AT&T employees, and potentially, the third-party hackers without his consent and without legitimate business reasons. On information and belief, this includes, but was not limited to, information about the configuration, type, and use of his subscribed AT&T services, his personal information, his SIM card details, and his

[17] Declaratory Ruling, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information & Other Customer Information*, 28 F.C.C. Rcd. 9609 ¶ 30 (2013) (hereafter, "2013 CPNI Order").
[18] 47 U.S.C. § 222(h)(1).

billing information. AT&T employees then used this information to effectuate an unauthorized SIM swap.

101. This type of unauthorized use of Mr. Williams' CPNI is illegal under the FCA. The FCA forbids AT&T from "us[ing], disclos[ing], or permit[ting] access to" CPNI, except in limited circumstances.[19] As AT&T has admitted, this extends to the carrier's own employees.

102. AT&T may only use, disclose, or permit access to Mr. Williams' CPNI: (1) as required by law; (2) with his approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service.[20] Beyond such use, "the Commission's rules require carriers to obtain a customer's knowing consent before using or disclosing CPNI."[21]

103. AT&T failed to protect Mr. Williams from authorized use of his CPNI. AT&T permitted its employees to use and/or disclose Mr. Williams' CPNI without obtaining Mr. Williams' knowing consent beforehand. AT&T employees, acting within the scope of their employment, purposefully and/or negligently, failed to seek Mr. Williams' knowing consent before using, disclosing, and/or permitting access to his CPNI when they accessed his account and swapped his SIM card. Because such conduct does not fit within the FCA's recognized legitimate uses, it constitutes a violation of the FCA.

104. Pursuant to the FCA, the FCC has developed comprehensive rules concerning AT&T's obligations under its duty to protect customers' CPNI.[22] This

[19] 47 U.S.C. § 222(c)(1).
[20] 47 U.S.C. § 222.
[21] 2007 CPNI Order ¶ 8 (emphasis added).
[22] *See* 47 C.F.R. § 64.2001("The purpose of the rules in this subpart is to implement section 222 of the Communications Act of 1934, *as amended*, 47 U.S.C. 222."). The FCC also regularly

includes rules "designed to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI."[23] The FCC specifically recognizes that "[a]bsent carriers' adoption of adequate security safeguards, consumers' sensitive information . . . can be disclosed to third parties without consumers' knowledge or consent."[24] In a 2013 order, the FCC "clarif[ied] existing law so that consumers will know that *their carriers must safeguard these kinds of information so long as the information is collected by or at the direction of the carrier and the carrier or its designee*[25] *has access to or control over the information*."[26]

105. Pursuant to these rules, AT&T must "implement a system by which the status of a customer's CPNI approval can be clearly established *prior to* the use of CPNI."[27] AT&T is also required to "design their customer service records in such a way that the status of a customer's CPNI approval can be clearly established."[28] The FCC's rules also "require carriers to maintain records that track access to customer CPNI records."[29]

106. Upon information and belief, AT&T has failed to implement such a system. The fact that Mr. Williams' account was accessed without his authorization on at least seven separate occasions demonstrates AT&T's failures in this regard.

---

releases CPNI orders that promulgate rules implementing its express statutory obligations. *See* 2007 CPNI Order & 2013 CPNI Order.

[23] 2007 CPNI Order ¶ 9; *see also id.* ¶ 35; 47 U.S.C. § 222(c); 47 C.F.R. § 64.2009.

[24] 2013 CPNI Order ¶ 1.

[25] In the ruling, "designee" is defined as "an entity to which the carrier has transmitted, or directed the transmission of, CPNI or is the carrier's agent." *Id.* n.1.

[26] *Id.* ¶ 1 (emphasis added).

[27] 2007 CPNI Order ¶¶ 8-9 (emphasis added); *see also* 47 C.F.R. § 64.2009(a).

[28] 2007 CPNI Order ¶ 9.

[29] *Id*.

107. AT&T is also required to "train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place."[30]

108. Upon information and belief, AT&T has failed to properly train and supervise their personnel, as reflected by AT&T personnel's involvement in Mr. Williams' breaches.

109. Carriers must "maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI."[31]

110. Upon information and belief, AT&T has failed to maintain such a record, as demonstrated by its repeated failure to protect Mr. Williams after his CPNI was provided to third-parties.

111. AT&T has also breached its duty to safeguard Mr. Williams' CPNI from data breaches, in violation of Section 222(a) and Section 201(b) of the FCA.

112. The FCC has "[made] clear that carriers' existing statutory obligations to protect their customers' CPNI include[s] a requirement that carriers take reasonable steps, which may include encryption, to protect their CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI."[32]

113. AT&T failed to take reasonable steps to protect Mr. Williams' CPNI, thereby allowing third party hackers to access his CPNI on at least seven occasions.

114. The FCC also requires that carriers inform customers—and law enforcement—"whenever a security breach results in that customer's CPNI being

[30] 47 C.F.R. § 64.2009(b).
[31] 47 C.F.R. § 64.2009(c).
[32] 2007 CPNI Order ¶ 36 (citation omitted).

disclosed to a third party without that customer's authorization."[33] This requirement extends to any unauthorized disclosure.

115. In adopting this requirement, the FCC rejected the argument that it "need not impose new rules about notice to customers of unauthorized disclosure because competitive market conditions will protect CPNI from unauthorized disclosure."[34]

116. Instead, the FCC found that "[i]f customers and law enforcement agencies are unaware of [unauthorized access], unauthorized releases of CPNI will have little impact on carriers' behavior, and thus provide little incentive for carriers to prevent further unauthorized releases. By mandating the notification process adopted here, we better empower consumers to make informed decisions about service providers and assist law enforcement with its investigations. This notice will also empower carriers and consumers to take whatever 'next steps' are appropriate in light of the customer's particular situation."[35] The FCC specifically recognized that this notice could allow consumers to take precautions or protect themselves "to avoid stalking or domestic violence."[36]

117. AT&T failed in its duty to safeguard Mr. Williams' CPNI from breaches and has failed to properly inform him of such breaches when they occurred. Mr. Williams never received any documentation or notice alerting him that his CPNI had been breached, despite being SIM swapped *seven* times.

118. Under the FCA, AT&T is not just liable for its own violations of the Act, but also for violations that it "cause[s] or permit[s]."[37] By failing to secure

[33] *Id.* ¶ 26; *see also* 47 C.F.R. § 64.2011(c).
[34] 2007 CPNI Order ¶ 30.
[35] *Id.*
[36] *Id.* at n.100.
[37] *See* 47 U.S.C.A. § 206 (establishing that "[i]n case any common carrier shall do, or cause or permit to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful,

Mr. Williams' account and protect his CPNI, AT&T caused and/or permitted Mr. Williams' CPNI to be accessed and used by its own employees and, subsequently, by third-party hackers.

119. AT&T is also responsible for the acts, omissions, and/or failures of officers, agents, employees, or any other person acting for or employed by AT&T, including employees Venessa (VL828B), Rex Mostoles (RX8927), and "Steve."[38]

E. Mr. Williams' Harm was Caused by AT&T's Negligence.

120. By failing to secure Mr. Williams' account—and protect the confidential and sensitive data contained therein—and to properly hire, train, and supervise their employees, AT&T is responsible for the foreseeable harm Mr. Williams suffered as a result of AT&T's negligence.

121. Further, AT&T is responsible for its employees' participation and/or gross negligence in the SIM swap attacks suffered by Mr. Williams, as such actions were within the scope of their employment with AT&T. On information and belief, AT&T employees were tasked with and able to change customers' SIM cards.

122. Additionally, AT&T employees' breach of Mr. Williams' account and the subsequent SIM swaps were foreseeable. AT&T knew or should have known that Mr. Williams' account was at risk, but nonetheless failed to secure his account and failed to properly supervise and train its employees.

123. AT&T employees continually ignored warnings in its system not to make changes to Mr. Williams' account.

124. AT&T has known for more than a decade that third parties frequently attempt to access wireless customers' accounts for fraudulent purposes. In 2007,

---

or shall omit to do any act, matter, or thing in this chapter required to be done, such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter[.]")

[38] 47 U.S.C. § 217.

the FCC issued an order strengthening its CPNI rules in response to the growing practice of "pretexting."[39] Pretexting is "the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communication records."[40] This 2007 Order put AT&T on notice that its customers' accounts were vulnerable targets of the third-parties seeking unauthorized access.

125. AT&T also knew, or should have known, about the risk SIM swap crimes presented to its customers. SIM swap crimes have been a widespread and growing problem for years. The U.S. Fair Trade Commission ("FTC") reported in 2016 that there were 1,038 reported SIM swap attacks *per month* in January 2013, which increased sharply to 2,658 per month by January 2016.[41] The FTC reported that SIM swaps represented 6.3% of all identity thefts reported to the agency in January 2016, and that such thefts "involved all four of the major mobile carriers" – including AT&T.[42]

126. AT&T knew or should have known that it needed to take steps to protect its customers. The FTC's 2017 Report stated that "*mobile carriers are in a better position than their customers to prevent identity theft through mobile account hijacking*[.]"[43] The FTC urged carriers like AT&T to "adopt a multi-level approach to authenticating both existing and new customers and require their own employees as well as third-party retailers to use it for all transactions."[44] The FTC

[39] 2007 CPNI Order.
[40] *Id.* ¶ 1.
[41] Lori Cranor, FTC Chief Technologist, *Your mobile phone account could be hijacked by an identity thief*, Federal Trade Commission (June 7, 2016), https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief (hereafter, "2017 FTC Report").
[42] *Id.*
[43] *Id.* (emphasis added).
[44] *Id.*

also specifically warned carriers like AT&T of the risk that, due to two-factor authentication, SIM swapping put subscribers at risk of financial loss and privacy violations:

> Having a mobile phone account hijacked can waste hours of a victim's time and cause them to miss important calls and messages. However, this crime is particularly problematic due to the growing use of text messages to mobile phones as part of authentication schemes for financial services and other accounts. The security of two-factor authentication schemes that use phones as one of the factors relies on the assumption that someone who steals your password has not also stolen your phone number. *Thus, mobile carriers and third-party retailers need to be vigilant in their authentication practices to avoid putting their customers at risk of major financial loss and having email, social network, and other accounts compromised.*[45]

127. AT&T admitted it was aware of SIM swap crimes and the effect they could have on its customers in September 2017 when AT&T's Vice President of Security Platforms published an article on AT&T's "Cyber Aware" blog about SIM swaps.[46] In the article, AT&T acknowledged that subscribers with "valuable accounts that are accessible online" are likely targets of SIM swaps. AT&T recommended that its customers set up passcodes that would provide "extra security."

128. AT&T informs its customers that these account passcodes—which are different than account sign-in passwords or the passcodes used to access a wireless device—are used to protect their wireless accounts and may be required when a

[45] *Id.* (emphasis added).
[46] Brian Rexroad, *Secure Your Number to Reduce SIM Swap Scams*, AT&T's Cyber Aware (Sept. 2017), https://about.att.com/pages/cyberaware/ni/blog/sim_swap.

customer manages their AT&T account online or in an AT&T store.[47] AT&T employees represented to Mr. Williams that this passcode would not be shared with anyone, and would protect his account from future unauthorized SIM swaps. Mr. Williams decided not to close his AT&T account in reliance on these assurances. These passcodes repeatedly failed to protect Mr. Williams.

129. AT&T therefore knew that its customers' accounts were at risk *at least* a year before *any* breaches of Mr. Williams' account. After the first attack on his phone in November 2018, Mr. Williams informed AT&T—both on the phone and in person—that he had valuable online accounts, thereby making him the type of individual that AT&T recognized was specifically vulnerable to SIM swap attacks. Nonetheless, AT&T failed to take reasonable steps to protect his account.

130. AT&T's inadequate security procedures are particularly egregious in light of AT&T's repeated public statements about the important of cyber security and its public representations about its expertise in this area. AT&T has an entire series on its public YouTube channel ("AT&T ThreatTraq") dedicated to discussing and analyzing emerging cybersecurity threats.[48] In its videos, AT&T describes itself as a "network that senses and mitigates cyber threats."[49]

131. AT&T recognizes the risks that arise when a cell phone is compromised, stating, "Our phones are mini-computers, and with so much personal data on our phones today, it's also important to secure our mobile devices."[50] AT&T's advertisements also stress how central a role cell phones play in its customer's lives, stating: "My phone is my life" and "My phone is

---

[47] *Get info on passcodes for wireless accounts*, AT&T, https://www.att.com/esupport/article.html#!/wireless/KM1049472?gsi=tp3wtr.
[48] *AT&T Tech Channel*, YouTube, https://www.youtube.com/user/ATTTechChannel.
[49] *AT&T – Protect Your Network with the Power of &*, VIMEO, https://vimeo.com/172399153.
[50] *AT&T Mobile Security*, YouTube (Feb. 12, 2019), https://www.youtube.com/watch?v=KSPHS89VnX0.

everything." The same ad stresses how the inability to use a cell phone makes people feel "completely untethered, flailing around."[51]

132. AT&T markets its ability to identify and to neutralize emerging cyber threats for its customers. In one video, AT&T employees discuss "threat hunting" which they describe as "an active threat analysis where you're actually thinking about your adversary."[52] They claim that it is "important" and "something [AT&T has] been doing for a long time."[53] They advise that companies think about "what would a hacker want to do, where would a hacker go to get my data, what are some of the points on my network that are most vulnerable, or where is the data flow that is potentially going to be a leakage" and state that "having threat hunting as part of a proactive continuous program, integrating with existing security measures, will help [you] stay ahead of the threats."[54] Not only did AT&T advise staying ahead of and addressing cyber threats, it also stressed that these practices could even help identify "insider threats"—employees within the company.

133. In an additional video focused on insider threats, AT&T employees go on at length about the threat of company insiders selling corporate information *and access*, citing a survey showing that "30% [of respondents] had purposefully sent data outside of their organization at some point in time" and "14% of the people that were interviewed said they would actually sell their corporate log-ins to folks on the outside or sell that data for less than about $250 US."[55] They cited as a "significant concern" the "individuals that have privileged access, that have broad

---

[51] *AT&T Mobile Movement Campaign – Ads*, VIMEO, https://vimeo.com/224936108.
[52] AT&T Tech Channel, *The Huntin' and Phishin' Episode*, YouTube (Apr. 21, 2017), https://www.youtube.com/watch?v=3g9cPCiFosk.
[53] *Id.*
[54] *Id.*
[55] AT&T ThreatTraq, *The Real Threat of Insider Threats*, YouTube (May 5, 2017), https://www.youtube.com/watch?v=ZM5tuNiVsjs.

access inside an organization."[56] AT&T therefore knew or should have known that there was a significant risk that its own employees would sell AT&T data—including customer account data—and that the risk was heightened when employees had too broad of access to corporate systems, yet failed to put sufficient systems and resources in place to mitigate that risk, despite its own advice to the contrary.

134. AT&T has also recognized the danger presented to its customers when their email addresses are hacked, as Mr. Williams' was on multiple occasions as a result of AT&T's failures. As one AT&T employee puts it: "I think most people do have something valuable [in their email accounts], which is access to all their other accounts, which you can get with a password reset."[57] They call this "something worth keeping safe."[58] "A strong, obviously, security awareness program within a company, I think, is extremely important."[59]

135. In this video series, AT&T makes specific mentions of SIM swapping activity. In one video, AT&T's Vice President of Security Platforms (Brian Rexroad) and Principal of Technology Security (Matt Keyser) discuss the hack of a forum called OGusers. [60] In the segment, they discuss the hacking of social media users' account names and point to a news story that highlights—in distinct orange type—that OGusers is a forum popular among people "conducting SIM swapping attacks to seize control over victims' phone numbers."[61]

---

[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] AT&T ThreatTraq, *5/31/19 Account-hacking Forum OGusers Hacked*, YouTube (May 31, 2019), https://www.youtube.com/watch?time_continue=234&v=cS4xV3cej3A.
[61] *Id.*

Figure 3

136. AT&T was therefore well aware of the significant risk that AT&T employees and SIM swapping presented to its customers, and the need to mitigate such risks, but nonetheless failed to take adequate steps to protect Mr. Williams.

Instead, it continued to make public statements giving rise to a reasonable expectation that AT&T could—and would—protect its customers.

137. The risk to Mr. Williams' account, specifically, was particularly foreseeable after the second breach on November 30, 2018. Despite their knowledge that this was the *second SIM SWAP attack in one month* and that he was getting death threats from the hackers, AT&T employees continually conducted SIM swaps, purposefully and/or negligently assisting the hackers. They ignored instructions in his account not to conduct changes unless the changes were requested in person from Mr. Williams, at a particular store, and only if Mr. Williams brought two passports. Instead, AT&T allowed his SIM card to be changed by unauthorized and nefarious hackers *seven* times. By conducting these unauthorized SIM swaps, AT&T employees aided hackers in stealing and

destroying almost $2 million worth of money, investments, and equipment from Mr. Williams.

138. Even after *two* documented account breaches and unauthorized SIM swaps in November, AT&T failed to protect Mr. Williams' account on *five* additional occasions between December 2018 and February 2019.

139. That Mr. Williams was at risk of account breaches at the hands of AT&T employees is particularly foreseeable—and AT&T's failures are particularly stark—in light of AT&T's history of unauthorized employee access to customer accounts.

140. In 2015, AT&T faced an FCC enforcement action, and paid a $25 million civil penalty, for nearly identical failures to protect its customers' sensitive account data.[62] In that case, as AT&T admitted, AT&T call center breached 280,000 customers' accounts.[63] Specifically, AT&T employees had improperly used login credentials to access customer accounts and access customer information that could be used to unlock the customers' devices.[64] The employees then sold the information they obtained from the breaches to a third party.[65]

141. The FCC concluded that AT&T's "failure to reasonably secure customers' proprietary information violates a carrier's statutory duty under the Communications Act to protect that information, and also constitutes an unjust and unreasonable practice in violation of the Act."[66]

142. The FCC stressed that the FCA is intended to "ensure that consumers can trust that carriers have taken appropriate steps to ensure that unauthorized

[62] *In the Matter of AT&T Servs., Inc.*, 30 F.C.C. Rcd. 2808 (2015).
[63] *Id.* ¶ 1.
[64] *Id.* ¶¶ 7, 11.
[65] *Id.* ¶ 1.
[66] *Id.* ¶ 2.

persons are not accessing, viewing or misusing their personal information."[67] It stressed its expectation that "telecommunications carriers such as AT&T… take 'every reasonable precaution' to protect their customers' data[.]"[68]

143. As a condition of its stipulated Consent Decree, AT&T agreed to develop and implement a compliance plan to ensure appropriate safeguards to protect consumers against similar breaches by improving its privacy and data security practices.[69]

144. This FCC enforcement action underscores AT&T's knowledge of the risk its employees presented to customers, the prevalence of employee breaches to customer data, the sensitive nature of customer CPNI, and its duties to protect and safeguard that data.

145. Nonetheless, more than 3 years later, AT&T still failed to protect its customer from employee breaches of customer CPNI and other account data, heightening the degree of its negligence.

i. AT&T is Liable for the Acts of its Employees.

146. AT&T is liable for the acts of its employees, including Mostoles, Vennessa and Steve, among others, who facilitated the unauthorized access to, and resulting theft from and privacy violations of, Mr. Williams.[70]

147. AT&T failed to put in place adequate systems and procedures to prevent the unauthorized employee access to and changes to Mr. Williams' account and related data. AT&T failed to properly hire and supervise its employees, allowing them to access Mr. Williams' sensitive and confidential account data,

[67] *Id.*
[68] *Id.*
[69] *Id.* ¶¶ 2, 17-18, 21.
[70] 47 U.S.C. § 217.

update his account without authorization, and give control of his account to third-party hackers.

148. In the context of AT&T's enterprise as a telecommunications carrier, an employee accessing a customer's account information and effectuating a SIM swap—even without authorization—is not so unusual or startling that it would not be unfair to include the loss resulting from such unauthorized access among other costs of AT&T's business, particularly in light of AT&T's awareness of the risk of SIM swaps to its customers.

149. Further, imposing liability on AT&T may prevent recurrence of SIM swap behavior because it creates a strong incentive for vigilance and proper safeguarding of customers' data by AT&T—which is the sole party in the position to guard substantially against this activity, as it is the custodian and guardian of this data.

150. As a customer of AT&T, Mr. Williams is entitled to rely upon the presumption that AT&T and the agents entrusted with the performance of AT&T's business have faithfully and honestly discharged the duty owed to him by AT&T, and that they would not gain unauthorized access to his account to purposefully and/or negligently aid in perpetuating a theft from him.

151. The reasonableness of Mr. Williams' expectations that AT&T would safeguard his data is confirmed by the fact that the federal agency responsible for overseeing AT&T's duties to its customers, the Federal Communications Commission ("FCC"), has stated that it "fully expect[s] carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information."[71]

[71] 2007 CPNI Order ¶ 64.

F. AT&T's Misrepresentations and Omissions.

152. AT&T's Privacy Policy, and the "Privacy Commitments" included therein, falsely represents and fails to disclose material information about its data security practices.

153. In its Privacy Policy, AT&T promised to protect Mr. Williams' privacy and personal information, including by using "security safeguards." AT&T further pledges that it will not sell customer data.

154. These representations created an expectation that Mr. Williams' AT&T account and associated data would be safe and secure, that employees would not access his account without authorization or sell access to his account, that his data would be protected from unauthorized disclosure, and that he could control how and when his data was accessed. Figure 4, immediately below, is an excerpt from AT&T's Privacy Policy.

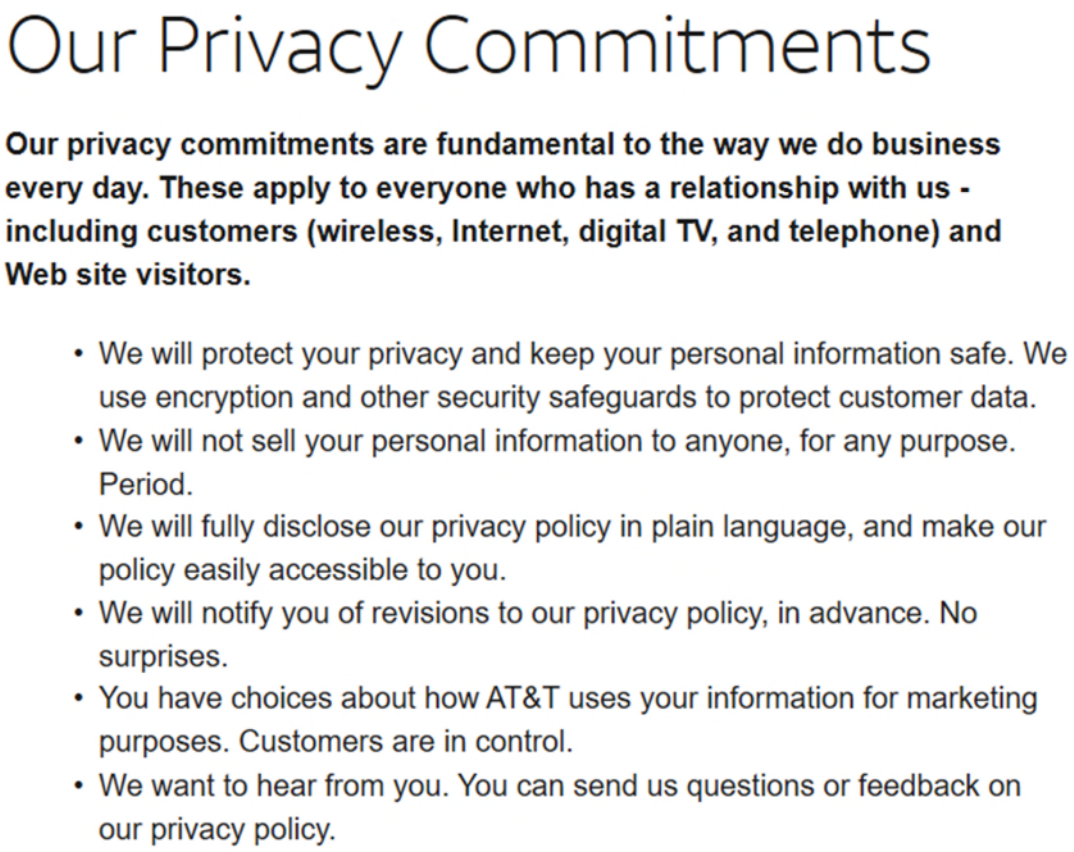

Figure 4[72]

155. AT&T's representation that it "uses encryption and other security safeguards to protect customer data" is false and misleading.

156. As alleged above, AT&T allowed its employees to access Mr. Williams' account, and the CPNI and other sensitive data contained therein, without his authorization. AT&T's statement that it would use encryption and other security safeguards to protect customers' data is therefore a material misrepresentation.

157. Upon information and belief, AT&T's security safeguards were inadequate, including its system which—upon information and belief—allowed an individual employee to conduct SIM swaps without adequate oversight, even when

[72] *Privacy Policy,* AT&T, attached hereto as Exhibit A.

there was warning and information on Mr. Williams' account not to conduct SIM swaps.

158. "Having one employee who can conduct these SIM swaps without any kind of oversight seems to be the real problem," says Lieutenant John Rose, a member of the California-based Regional Enforcement Allied Computer Team ("REACT"), a multi-jurisdictional law enforcement partnership specializing in cybercrime.[73] "And it seems like [the carriers] could really put a stop to it if there were more checks and balances to prevent that. It's still very, very easy to SIM swap, and something has to be done because it's just too simple. Someone needs to light a fire under some folks to get these protections put in place."

159. AT&T failed to put in place adequate systems and procedures to prevent the unauthorized employee access to and changes to Mr. Williams' account and related data.

160. Additionally, as alleged above, AT&T failed to establish a consent mechanism that verified proper authorization before Mr. Williams' data was accessed and provided to third parties. AT&T's statement that it would use encryption and other security safeguards to protect customers' data is therefore a material misrepresentation.

161. AT&T's representation that it "will protect [customers'] privacy and keep [their] personal information safe" is false and misleading.

162. As alleged above, AT&T failed to establish a consent mechanism that verified proper authorization before Mr. Williams' account and the data therein was used without his authorization or consent, and disclosed to third parties. Mr.

[73] Busting SIM Swappers and SIM Swap Myths," KREBSONSECURITY (Nov. 18, 2018), *available at https://krebsonsecurity.com/2018/11/busting-sim-swappers-and-sim-swap-myths.*

Williams' privacy and personal information was not safe, as demonstrated by the repeated breaches of his AT&T account. AT&T's statement that it would protect customers' privacy and keep their personal information safe is therefore a material misrepresentation.

163. AT&T also makes numerous false or misleading representations concerning its treatment of customers' data that qualifies as CPNI under the FCA.

164. AT&T explicitly and falsely represents in its Privacy Policy that it does not "sell, trade or share" their CPNI:

> We do not sell, trade or share your CPNI with anyone outside of the AT&T family of companies* or our authorized agents, unless required by law (example: a court order).[74]

165. As alleged above, AT&T provided access to Mr. Williams' CPNI. This use was not required by law and was instead *prohibited* by law.

166. AT&T also states that it only uses CPNI "internally" and its *only* disclosed use of CPNI is "among the AT&T companies and our agents in order to offer you new or enhanced services."[75]

167. AT&T employees' unauthorized access to Mr. Williams's account and related data as described herein was not for "internal" AT&T purposes, nor was it used to market AT&T services. AT&T's statements regarding the use of customer CPNI are therefore material misrepresentations. Its failure to disclose this use and access to CPNI is a material omission.

[74] Exhibit A at 31-32. The "AT&T family of companies" is defined as "those companies that provide voice, video and broadband-related products and/or services domestically and internationally, including the AT&T local and long distance companies, AT&T Corp., AT&T Mobility, DIRECTV, and other subsidiaries or affiliates of AT&T Inc. that provide, design, market, or sell these products and/or services." *Id.*

[75] *Id.*

168. AT&T also falsely represents that it "uses technology and security features, and strict policy guidelines with ourselves and our agents, to safeguard the privacy of CPNI."

169. As alleged above, AT&T and its agents failed to safeguard Mr. Williams' CPNI. Instead, it stored customer CPNI in such a way that unauthorized access was easily obtained by an employee. AT&T's statements regarding the technology and security features it uses to safeguard customer CPNI are therefore material misrepresentations.

170. After each breach of his account and unauthorized SIM swap, AT&T repeatedly, and falsely, represented to Mr. Williams that his account was safe from future breaches. In reliance upon these statements, Mr. Williams maintained his AT&T account . AT&T also repeatedly told Mr. Williams that the notations made on his account and the passcode needed to change his SIM card would protect him from future breaches and SIM swaps. These misrepresentations were false and materially misleading, as demonstrated by the ongoing breaches to Mr. Williams' account.

171. AT&T was obligated to disclose the weaknesses and failures of its account and data security practices, as AT&T had exclusive knowledge of material facts not known or knowable to its customers, AT&T actively concealed these material facts from Mr. Williams, and such disclosures were necessary to materially qualify its representations that it did not sell and took measures to protect consumer data and its partial disclosures concerning its use of customers' CPNI. Further, AT&T was obligated to disclose its practices under the FCA.

172. A reasonable person would be deceived and misled by AT&T's misrepresentations, which clearly indicated that AT&T would not sell, and would in fact safeguard, its customers' personal information and CPNI.

173. AT&T intentionally misled Mr. Williams regarding its data security practices in order to maintain his business, make money off his account, and evade prosecution for its unlawful acts.

174. AT&T's representations that it protected customers' personal information, when in fact it did not, were false, deceptive, and misleading and therefore a violation of Section 201(b) of the FCA.

V. CLAIMS FOR RELIEF

COUNT I

Violations of The Federal Communications Act, 47 U.S.C. § 201 *et seq.*

175. Plaintiff Mr. Williams realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

176. AT&T has violated 47 U.S.C. § 222(a) by failing to protect the confidentiality of Mr. Williams' CPNI.

177. AT&T has violated 47 U.S.C. § 222(c) by using, disclosing, and/or permitting access to Mr. Williams' CPNI without the notice, consent, and/or legal authorization required under the FCA, as detailed herein. AT&T also caused and/or permitted third parties to use, disclose, and/or permit access to Mr. Williams' CPNI without the notice, consent, and/or legal authorization required under the FCA, as detailed herein.

178. Mr. Williams has suffered injury to his person, property, health, and/or reputation as a consequence of AT&T's violations of the FCA. He has suffered financial loss. He has not been able to start cryptocurrency mining again since the attack in November 2018. Additionally, Mr. Williams has suffered emotional damages, including personal humiliation, mental anguish, and suffering as a result of AT&T's acts and practices.

179. Mr. Williams seeks the full amount of damages sustained as a consequence of AT&T's violations of the FCA, together with reasonable attorney's

fee, to be fixed by the Court and taxed and collected as part of the costs of the case. Mr. Williams also moves for a writ of injunction or other proper process, mandatory or otherwise, to restrain Defendant AT&T and its officers, agents, or representatives from further disobedience of the 2007 and 2013 CPNI Orders, or to enjoin their obedience to the same.

COUNT II
Violation of North Carolina Unfair and Deceptive Trade Practices Act
N.C. Gen. Stat. Ann. § 75-1.1

180. Plaintiff Mr. Williams realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

181. AT&T committed unfair and deceptive acts and trade practices as set forth above.

182. North Carolina's Unfair and Deceptive Trade Practices Act ("NCUDTPA") prohibits any "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."

183. AT&T made material misrepresentations and omissions concerning its sale of access to and safeguarding of Mr. Williams' CPNI, constituting a deceptive practice under the NCUDPTA. As alleged above, a reasonable person would attach importance to the privacy of his sensitive location data in determining whether to contract with a wireless cell phone provider.

184. AT&T had a duty to disclose the nature of its inadequate security practices and failures in hiring, training, and supervising staff. AT&T had exclusive knowledge of material facts not known or knowable to its customers and AT&T actively concealed these material facts from its customers. Further, additional disclosures were necessary to materially qualify its representations that it took measures to protect that data, and its partial disclosures concerning its use of customers' CPNI. AT&T was obligated to disclose its practices, as required by

the NCUDTPA. The magnitude of the harm suffered by Mr. Williams, both financially and emotionally, underscores the materiality of the AT&T's omissions.

185. A reasonable person, such as Mr. Williams, would be deceived and misled by AT&T's misrepresentations, which indicated that AT&T would not sell, and would in fact safeguard, its customers' personal and proprietary information. A reasonable person, such as Mr. Williams, would also be deceived and misled by AT&T's misrepresentations regarding making changes to his account, which indicated that AT&T would not make changes to Mr. Williams' account without specific factors being fulfilled. The reasonableness of that expectation is heightened here, where AT&T purported to disclose the uses for which it accessed customers' CPNI but failed to include the security risks described here, making its partial representations likely to mislead or deceive.

186. AT&T intentionally misled its customers regarding its data protection practices in order to attract customers and evade prosecution for its unlawful acts. Indeed, AT&T told Mr. Williams after each SIM swap attack that his account would be safe from future breaches, and in reliance on those assurances, Mr. Williams did not close his AT&T wireless account.

187. AT&T's actions detailed herein constitute an unfair or deceptive trade practice under the NCUDTPA.

188. Defendants' actions as set forth above were in or affecting commerce.

189. These unfair and deceptive acts were immoral, substantially injurious, deceptive, unethical, and/or oppressive.

190. These unfair and deceptive acts and trade practices have caused damages to Mr. Williams to be proven at trial.

191. Mr. Williams is entitled to recover treble damages pursuant to N.C. Gen Stat § 75-16 and attorneys' fees pursuant to N.C. Gen. Stat. § 75-16.1

COUNT III
Negligence

192. Mr. Williams realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

193. AT&T owed a duty to Mr. Williams—arising from the sensitivity of his AT&T account information and the foreseeability of harm to Mr. Williams should AT&T fail to safeguard and protect such data—to exercise reasonable care in safeguarding his sensitive personal information. This duty included, among other things, designing, maintaining, monitoring, and testing AT&T's and its agents', partners', and independent contractors' systems, protocols, and practices to ensure that Mr. Williams' information was adequately secured from unauthorized access.

194. Federal law and regulations, as well as AT&T's privacy policy, acknowledge AT&T's duty to adequately protect Mr. Williams' confidential account information.

195. AT&T owed a duty to Mr. Williams to protect his sensitive account data from unauthorized use, access, or disclosure. This included a duty to ensure that his CPNI was only used, accessed, or disclosed with proper consent.

196. AT&T owed a duty to Mr. Williams to implement a system to safeguard against and detect unauthorized access to Mr. Williams' AT&T data in a timely manner.

197. AT&T owed a duty to Mr. Williams to disclose the material fact that its data security practices were inadequate to safeguard Mr. Williams' AT&T account data from unauthorized access by its own employees and others.

198. AT&T had a special relationship with Mr. Williams due to its status as his telecommunications carrier, which provided an independent duty of

care. AT&T had the unique ability to protect its systems and the data it stored thereon from unauthorized access.

199. Mr. Williams' willingness to contract with AT&T, and thereby entrust AT&T with his confidential and sensitive account data, was predicated on the understanding that AT&T would undertake adequate security and consent precautions.

200. AT&T breached its duties by, *inter alia*: (a) failing to implement and maintain adequate security practices to safeguard Mr. Williams' AT&T account and data—including his CPNI—from unauthorized access, as detailed herein; (b) failing to detect unauthorized accesses in a timely manner; (c) failing to disclose that AT&T's data security practices were inadequate to safeguard Mr. Williams' data; (d) failing to supervise its employees and prevent employees from accessing and utilizing Mr. Williams' AT&T account and data without authorization; and (e) failing to provide adequate and timely notice of unauthorized access.

201. But for AT&T's breaches of its duties, Mr. Williams' data would not have been accessed by unauthorized individuals.

202. Mr. Williams was a foreseeable victim of AT&T's inadequate data security practices and consent mechanisms. As alleged above, AT&T knew or should have known that SIM swaps presented a serious threat to its customers, including Mr. Williams, before Mr. Williams' account was breached for the first time. AT&T also knew or should have known that Mr. Williams was at a heightened risk after (1) he informed AT&T employees that he had digital currency accounts, a risk factor AT&T has acknowledged, and (2) he had previously been the target of SIM swap attacks. AT&T also knew that improper procedures and systems to safeguard customer data could allow its employees to authorize customers' accounts and data and sell that to third parties, as occurred in the 2015 FCC enforcement action.

203. AT&T knew or should have known that unauthorized accesses would cause damage to Mr. Williams. AT&T admitted that unauthorized account access presents a significant threat to its customers, and became aware during its 2015 FCC enforcement action of the harms caused by unauthorized account access.

204. AT&T's negligent conduct provided a means for unauthorized individuals to access Mr. Williams' AT&T account data, take over control of his wireless phone, and use such access to hack into numerous online accounts in order to rob Mr. Williams and steal his personal information.

205. As a result of AT&T's failure to prevent unauthorized accesses, Mr. Williams suffered grave injury, as detailed above. The damages Mr. Williams suffered were a proximate, reasonably foreseeable result of AT&T's breaches of its duties.

206. Therefore, Mr. Williams is entitled to damages in an amount to be proven at trial.

COUNT IV
Negligent Supervision

207. Mr. Williams realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

208. AT&T conducts its business activities through employees or other agents, including AT&T contract attorneys.

209. AT&T is liable for harm resulting from its agents' and employees' because AT&T was reckless or negligent in employing and/or entrusting employees—including, but not limited to, Vennessa, Steve, and Mostoles—in work involving the risk of harm to others, including Mr. Williams.

210. On information and belief, AT&T knew or had reason to believe that its employees—including Vennessa, Steve, and Mostoles—were unfit and failed to exercise reasonable care in conducting changes to Mr. Williams' account. AT&T

was negligent in supervising these employees and in entrusting them with what it knew to be highly sensitive confidential information. AT&T knew or had reason to know that its employees—including, but not limited to, Vennessa, Steve, and Mostoles —were likely to harm others in view of the work AT&T entrusted to them.

211. AT&T failed to exercise due care in selecting its employees, and thereby negligently or reckless employed Vennessa, Steve, and Mostoles, among others, to do acts—including accessing customer accounts and effectuating SIM swaps—which necessarily brought them in contact with others, including Mr. Williams, while in the performance of those duties.

212. AT&T's acts, as alleged herein, were negligent in that they created the risk of criminal acts.

213. Unauthorized account access and SIM swapping, the particular risks and hazards that Mr. Williams was exposed to, are tied to AT&T's negligence and recklessness in employing, and continuing to employee through the time of Mr. Williams' injury, Vennessa, Steve, and Mostoles, among other employees.

214. AT&T was or should have been on notice that its employees, including, but not limited to, Vennessa, Steve, and Mostoles, were acting negligently by conducting unauthorized SIM swaps.

215. AT&T also failed to properly supervise its employees, and instead continued to negligently entrust them with sensitive customer data. Had AT&T fired or disciplined Vennessa, Steve, and Mostoles, and other employees, when they conducted SIM swaps without authorization—including but not limited initiating an irregularly high number of SIM swaps in Mr. Williams' account in a short period of time—Mr. Williams would not have been injured.

216. Had AT&T built a system to effectively authenticate and verify consumer consent before allowing employees to access their CPNI—as required by the FCA—Mr. Williams would not have been injured.

217. Had AT&T prevent individual employees from unilaterally changing customer's SIM swaps without proper oversight, Mr. Williams would not have been injured.

218. In sum, AT&T gave its employees the tools and opportunities they needed to gain unauthorized access to Mr. Williams' account and failed to prevent them from doing so, thereby allowing them to use AT&T's systems to perpetuate privacy breaches and thefts against Mr. Williams.

219. Vennessa, Steve, and Mostoles, and other employees' actions have a causal nexus to their employment. Mr. Williams' injuries arose out of his contract with AT&T as his carrier, and AT&T's resulting access to his CPNI and account data as a result. The risk of injury to Mr. Williams was inherent in the AT&T working environment.

220. Mr. Williams' injury was also foreseeable. As established above, AT&T was aware of the risks that SIM swaps presented to their customers. AT&T was also aware that its customers' accounts were vulnerable to unauthorized access to and sale by its own employees, as demonstrated in the 2015 FCC enforcement action. AT&T was aware that Mr. Williams was at a heightened risk due to his involvement with cryptocurrency.

COUNT V
North Carolina's Anti-Hacking Statute
N.C.G.S.A. § 1-539.2A

221. Mr. Williams realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

222. North Carolina's Anti-Hacking statute prohibits "any person to use a computer or computer network without authority and with intent to. . . [t]emporarily or permanently remove, halt, or otherwise disable any computer data, computer programs, or computer software from a computer or computer network; [c]ause physical injury to the property of another; or [m]ake or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network.

223. Per this statute, "a person is 'without authority' when … the person has no right or permission of the owner to use a computer, or the person uses a computer in a manner exceeding the right or permission . . . ."

224. AT&T, through its employees, used a computer or computer network with the intent to disable and halt data from Mr. Williams's mobile device.

225. Further, AT&T, through its employees, made or caused to be made copies of Mr. Williams' confidential data by conducting a SIM swap and purposefully and/or negligently allowing and/or assisting third-party hackers to access and use his confidential data.

226. AT&T, through its employees, was not authorized by Mr. Williams to make such changes, yet did so. These employees, including, Vennessa, Steve, and Mostoles, ignored instructions telling them not to conduct a SIM swap unless certain conditions were met, and yet they purposefully and/or negligently ignored those instructions.

227. As a direct and proximate result of AT&T's actions, Mr. Williams has sustained monetary losses in the form of lost revenues and profits, as well as costs to restore data altered and/or deleted by the Defendant. Mr. Williams is therefore, entitled to have and recover compensatory damages in amounts to be proved at trial from Defendant.

COUNT VI
Violation of the Computer Fraud and Abuse Act
18 United States Code § 1030

228. Mr. Williams realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

229. Mr. Williams' mobile device is capable of connecting to the Internet.

230. AT&T employees, including Vennessa, Steve, and Mostoles, in the scope of their employment, accessed Mr. Williams' mobile device, and intentionally and/or negligently assisted others in accessing his mobile device, without Mr. Williams' authorization, in order to assist hackers into stealing cryptocurrency.

231. The AT&T employees, including Vennessa, Steve, and Mostoles, by taking these actions, knew or should have known, that they would cause damage to Mr. Williams' mobile device, as well as damage to the information located on his mobile device.

232. The AT&T employees, including Vennessa, Steve, and Mostoles, caused Mr. Williams' mobile device and much of the data on it to be unusable to him, including his Gmail, Slush Pool, and Coinbase accounts.

233. Because of the AT&T employees' actions, Mr. Williams suffered damage to his mobile device and damage to information on his mobile device, including being unable to access information and data on his mobile device and being unable to access his personal accounts, including his Gmail, HItBTC, Coinbase, Gemini, Twitter, and Slush Pool accounts.

234. The action of swapping a SIM card was in the scope of the AT&T employees' work.

235. Further, Mr. Williams spent in excess of $5,000 investigating who accessed his mobile device and damaged information on it.

VI. PRAYER FOR RELIEF

236. WHEREFORE, Plaintiff Jason Williams requests that judgment be entered against Defendants and that the Court grant the following:

A. Judgment against Defendants for Plaintiff's asserted causes of action;

B. Public injunctive relief requiring cessation of Defendants' acts and practices complained of herein pursuant to 47 U.S.C. § 401(b);

C. Pre- and post-judgment interest, as allowed by law;

D. An award of monetary damages, including punitive damages;

E. Reasonable attorneys' fees and costs reasonably incurred, including but not limited to attorneys' fees and costs pursuant to 47 U.S.C.A. § 206; and

F. Any and all other and further relief to which Plaintiff may be entitled.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all issues so triable.

Dated: October 24, 2019

Respectfully submitted,

/s/ Terence S. Reynolds

Terence S. Reynolds
treynolds@shumaker.com
NC State Bar No. 49848
Lucas D. Garber
lgarber@shumaker.com
NC State Bar No. 47756
SHUMAKER LOOP & KENDRICK LLP
101 South Tyron Street
Suite 2200
Charlotte, North Carolina 28280
Telephone: (704) 375-0057
Facsimile: (704) 332-1197
Local Civil Rule 83.1(d) Counsel for Plaintiff Jason Williams

Christopher N. LaVigne
clavigne@piercebainbridge.com
State Bar No. NY 4811121
Dwayne Sam
dsam@piercebainbridge.com
State Bar No. DC 1029785
Sarah Baugh
sbaugh@piercebainbridge.com
State Bar No. NY 5495957
Thomas Popejoy
tlpopejoy@piercebainbridge.com
State Bar No. NY 5444146
PIERCE BAINBRIDGE BECK PRICE & HECHT LLP
277 Park Avenue, 45th Floor
New York, NY 10172
Telephone: (212) 484-9866
Facsimile: (646) 968-4125
(pro hac vice forthcoming)
Counsel for Plaintiff Jason Williams